



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/949,525	10/14/1997	MICHAEL J. WIENER	ENT970827-1	8206

7590 03/13/2003

CHRISTOPHER J RECKAMP  
Vedder Price Kaufman & Kammholz  
222 North LaSalle Street  
Suite 2600  
Chicago, IL 60601

EXAMINER	
MEISLAHN, DOUGLAS J	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

08/949,525

Applicant(s)

WIENER ET AL.

Examiner

Douglas J. Meislahn

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 January 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                  | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____  |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)         | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

1. This action is in response to the amendment filed 13 January 2003 that added claim 30.

#### ***Response to Arguments***

2. Applicant's arguments filed 13 January 2003 have been fully considered but they are not persuasive.
3. Applicant is of the opinion that the cited references do not show selectable private key validity periods. The validity period selected in Ellison reads on selecting a validity period for both a private key and public key. This would not be the case if the two periods were different. This limitation would not necessarily render the claims allowable, but it would, at the very least, require the addition of a reference.
4. Applicant contends that Ellison teaches away from various aspects of the claims. However, the teaching on which the rejection relies is applicable to systems beyond that which Ellison discusses. The utility of this feature is obvious to a person of ordinary skill in the art, as suggested by Ellison referring to it as a matter of normal risk management.
5. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a

reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-4, 6, 8-18, 20-24, and 26-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (5761306) in view of Ellison (Generalized Certificates).

Lewis shows a public key replacement system. Figure 2 shows that both private and public keys are updated. Lewis' system causes a key switch. Lewis does not say that there are certificates with expiry data that is user selectable. Ellison talks throughout his disclosure about certificates, which are used to authenticate public keys. Certification authorities issue these certificates. On page five, Ellison says that he believes that there is a problem with CRLs. He believes, as he says in the paragraph bridging pages five and six, certificates should each include a validity field. He goes on to say that "[i]t is up to you to decide how long you're willing to have an invalid certificate out in the world – and to define the validity period accordingly. This is a matter of normal risk management." An e-mail message that begins on page seven and ends on page 9 of Ellison's article outlines the benefits of eliminating CRLs. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was

made to give users the ability to define the validity period for certificates, as taught by Ellison, in the public key distribution system of Lewis.

Lewis anticipates additional material in claim 9. Ellison shows claim 2. Claim 3 is met by Lewis in lines 64-65 of column 7. Claim 6 is inherent to Ellison in that an interface to select validity periods is required.

8. Claims 5, 19, 25, and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Ellison as applied to claims 1, 14, and 21 above, and further in view of applicant's admitted prior art.

Lewis and Ellison teach the selection of key validity periods on a per client basis. They do not specify a time frame in which a client can request key updates. In lines 14 through 19 of page 2, applicant discusses a conventional public key system in which keys have a fixed default period that is "... generally a fixed percentage or a total key lifetime . . . ." Official notice is taken that fixed length renewal periods are old and well known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to set key update periods that are based on a fixed number of days and a percentage of a key's lifetime. This method provides flexibility by giving clients who have keys that have either extremely long or extremely short lifetimes two options as to when to update their keys.

9. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Ellison as applied to claim 1 above.

Lewis and Ellison teach the selection of key validity periods on a per client basis. In their system, keys are created by a user and then sent to a certification authority for a

certificate. In another implementation of public-key cryptosystems, the certification authority both generates and verifies the public/private key pair, sometimes on request. The previously mentioned RSA key marketing method exemplifies this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teachings of Lewis and particularly Ellison to the well-known public key cryptosystem where a certification authority produces the key pair.

10. Claims 1-4, 6, 8-18, 20-24, and 26-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. (6003014) in view of Ellison.

Looking at claim 30, in lines 49-65 of column 10, Lee et al. teach sending an issuer's public/private key pair (IPK/ISK) to a certificate authority (CA). The CA generates a certificate (ICERT) using its private key (CASK). The issuer reads on applicant's client, and the transmission of IPK and ISK reads on applicant's digital signature key pair. The CA would not generate ICERT if it had not determined that it was requested to do so, with the reception of the key pair reading on the request and the reception. As described in lines 13-18 of column 11, ICERT includes information identifying the issuer and expiry information. As implied in the following paragraph, ICERT contains the CA's signature and the issuer's public key. As such the last clause of claim 30 is met. Lee et al. do not say that the expiry data is selectable. In the paragraph spanning pages 5 and 6, Ellison teaches setting public key validity periods according to risk management. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for Lee et al.'s validity periods to be selectable, as taught by Ellison, in order to allow for risk management. As the CA

produces the certificates in Lee et al., it would be obvious for the CA to provide, and necessary for it to store, the expiry information. The existence of expiry information renders obvious new and old key pairs and the necessary transfer between the two.

Claims 1, 9, 14, and 21 contain subject matter similar to, but broader than, that covered by claim 30 and are rejected for largely the same reasons. The rationale behind the rejections of the dependent claims are apparent from either their similarity to claim 30 or features of the prior art discussed in preceding paragraphs.

11. Claims 5, 19, 25, and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. and Ellison as applied to claims 1, 14, and 21 above, and further in view of applicant's admitted prior art.

Lee et al. and Ellison teach the selection of key validity periods on a per client basis. They do not specify a time frame in which a client can request key updates. In lines 14 through 19 of page 2, applicant discusses a conventional public key system in which keys have a fixed default period that is "... generally a fixed percentage or a total key lifetime . . . ." Official notice is taken that fixed length renewal periods are old and well known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to set key update periods that are based on a fixed number of days and a percentage of a key's lifetime. This method provides flexibility by giving clients who have keys that have either extremely long or extremely short lifetimes two options as to when to update their keys.

12. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. and Ellison as applied to claim 1 above.

Lee et al. and Ellison teach the selection of key validity periods on a per client basis. In their system, keys are created by a user and then sent to a certification authority for a certificate. In another implementation of public-key cryptosystems, the certification authority both generates and verifies the public/private key pair, sometimes on request. The previously mentioned RSA key marketing method exemplifies this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teachings of Lee et al. and particularly Ellison to the well-known public key cryptosystem where a certification authority produces the key pair.

### ***Conclusion***

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Asay et al. – section 1.B.14, starting at line 56 of column 27; Brennan et al. (5675649) – lines 22-31 of column 12.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.



Art Unit: 2132

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



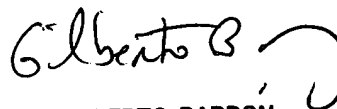
DJM

March 7, 2003

Douglas J. Meislahn

Examiner

Art Unit 2132



GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100